ORIGIN DS-00

INFO	LOG-00	MFA-00	EEB-00	AF-00	CIAE-00	CTME-00	INL-00
	DNI-00	DODE-00	DOTE-00	WHA-00	PERC-00	EAP-00	DHSE-00
	EUR-00	OIGO-00	FAAE-00	FO-00	TEDE-00	INR-00	IO-00
	MFLO-00	MMP-00	MOFM-00	MOF-00	NEA-00	DCP-00	NSCE-00
	OIC-00	OIG-00	PA-00	DOHS-00	FMPC-00	SP-00	IRM-00
	SSO-00	SS-00	DPM-00	USSS-00	CBP-00	R-00	SHEM-00
	DSCC-00	SCA-00	SAS-00	FA-00	/000R		

118905
SOURCE: CBLEXCLS.004960
DRAFTED BY: DS/DSS/CC:JBACIGALUPO -- 11/07/2008 571-345-3132
APPROVED BY: DS/DSS/CC:JBACIGALUPO
------------------F72CB3 071658Z /38
P 071648Z NOV 08
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG

S E C R E T STATE 118905

NOFORN

E.O. 12958: DECL: MR
TAGS: ASEC
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple Sources

SECRET//NOFORN//MR
Declassify on: Source marked 25X1-human, Date of source:
November 6, 2008

¶1. (U) Diplomatic Security Daily, November 7, 2008

¶2. (U) Significant Events) Paragraphs 5-8

¶3. (U) Key Concerns) Paragraphs 9-24

¶4. (U) Cyber Threats) Paragraphs 25-32

¶5. (U) Significant Events

¶6. (SBU) AF - Guinea - Emergency Action Committee (EAC) Conakry convened November 6 to review the U.S. Embassy,s security posture. The committee decided to remove travel limitations during daylight hours for Mission staff, continuing to ensure all employee travel during nighttime hours is conducted with prior RSO concurrence. Post will maintain increased security patrols around residences, facilities, and vehicle routes used by Mission staff. No direct threat to American or foreign citizens has occurred. (Conakry 0680)

¶7. (SBU) EAP - New Zealand - Approximately 24 individuals arrived at U.S. Embassy Wellington November 6 to peacefully protest the war in Iraq. The individuals gathered outside the front gate. New Zealand police presence was adequate, and all necessary Mission security measures were in place for this event. The protest ended without incident. (RSO Wellington Spot Report)

¶8. (S//NF) SCA - Pakistan - EAC Peshawar convened November 5 to discuss threat reporting and recent incidents within the Peshawar area affecting U.S. Consulate operations. There have been several incidents within 2 km of Mission residential and off-compound facilities in recent days. On November 1, an explosion at a Peshawar police substation killed one police officer and injured several others. On November 3 and 4, several explosions occurred on the airfield serving Peshawar International Airport and Pakistani Air Force Ninth Aviation. The EAC concluded that current threat reporting and recent incidents warrant continuation of Post,s heightened security

posture. (Appendix source 1)

¶9. (U) Key Concerns

¶10. (SBU) EUR - Hungary - Bomb threats include U.S. Embassy Budapest: On November 6 at approximately 12:20 p.m., the Hungarian police notified RSO Budapest that the U.S. Embassy was mentioned in a telephonic bomb threat called in to the Budapest ambulance service. A female caller speaking in Hungarian warned of the bomb and gave her name, but provided no further information; police believe the name given by the caller is a fake identity. Embassy Budapest local guards, Marine guards, and RSO personnel conducted a sweep of all common access spaces and Post,s perimeter security zone, and a police explosive ordnance disposal dog team and bomb technicians conducted a sweep of the perimeter and adjacent vehicles; no suspicious devices were discovered. Two additional telephonic bomb threats were made against Hungarian Government (HG) offices the same day -- Budapest,s Fourth District Police headquarters and the governing Hungarian Socialist Party,s (MSZP,s) office, also in the Fourth District; a sweep revealed an unexploded pipe bomb at the MSZP building, just two weeks after the discovery of a hand grenade at the same site. DS/TIA/ITA notes there is no information indicating any specific reason for a threat to the Embassy. As for the threat against the government and police, for the past two years, right-wing extremist groups have demonstrated violently against the governing party and its party members over domestic political issues, using such tactics as Molotov cocktails and other incendiary devices, burning cars, and once ransacking the Hungarian Television building. Threat information and anti-HG activity peaked in late October, the commemoration of the 1956 Hungarian Revolution; although, demonstration activity was far less than experienced during the previous two Octobers. To date, the USG has remained mostly separated from the fray, but for the proximity of Embassy Budapest to the Hungarian Parliament and several controversial memorials. Post and parliament are both located in the Fifth District of central Budapest, several miles south of the Fourth District (jpest). (Open sources; Budapest 1064)

¶11. (S//NF) AF - Mali - Belmokhtar learns of U.S. troops arrival: Tearline from November 6 reads, &Al-Qa,ida in the Lands of the Islamic Maghreb (AQIM) leader Mokhtar Belmokhtar was aware that American, British, and German troops had arrived in Mali on November 5. Belmokhtar discovered that the troops had two helicopters, and they were there to conduct training in Timbuktu and Gao.8

¶12. (S//NF) A body of previous tearline from over the last several months has also highlighted Belmokhtar,s and AQIM,s monitoring of U.S. troops in northern Mali. DS/TIA/ITA suspects their interest in the troop movements and whereabouts likely stems from a desire to practice operational security, rather than to attack them. Although two recent reports, stemming from firsthand sources claiming regular and irregular access, detailed AQIM,s alleged plans to attack U.S. troops if they conducted reconnaissance north of Timbuktu, DS/TIA/ITA judges that it would not be in the best interest of AQIM or Belmokhtar to pursue such actions. Doing so would bring increased international scrutiny on a region which AQIM uses as a safehaven and recruiting/logistics/training point for larger attacks in Algeria. (Appendix sources 2-4)

¶13. (S//NF) NEA - Lebanon - Plan to carry out suicide attacks against LAF and UNIFIL in Lebanon:

¶14. (S//NF) According to sensitive reporting from late October, Fatah al-Islam and Jund Al-Sham members in the Ayn Al-Hilwah camp held a series of meetings to plan attacks against unspecified Lebanese Armed Forces (LAF) and United Nations Interim Forces in Lebanon (UNIFIL) targets in southern Lebanon and Beirut. During the meeting, attendees reportedly agreed to use vehicle-borne improvised explosive devices (VBIEDs), explosive belts, and IEDs in the attacks. The report also alleges a Fatah al-Islam and a Jund Al-Sham

member worked together to dismantle approximately 30 land mines to extract the TNT, which they separated into 5 kg packages.

¶15. (S//NF) DS/TIA/ITA notes this is the latest in a handful of recent reports regarding Islamic extremists in the Ayn Al-Hilwah camp plotting against the LAF, UNIFIL, and other foreign interests in Lebanon. Recently, Islamic extremist groups in the camp were preoccupied with settling disputes among themselves, which put plans to carry out terrorist attacks on the back burner. While the disputes between the groups -- particularly Jund Al-Sham and the Palestinian Fatah -- reportedly are not completely resolved, the groups do appear to be refocusing on their reason for being, which is conducting Jihad by carrying out attacks against the LAF and foreign interests in-country. (Appendix source 5)

¶16. (S//NF) SCA - Afghanistan - Al-Qa,ida plans suicide bombing against embassies of the U.S., Germany, and Denmark: An Arab al-Qa,ida associate in Pakistan named Haji Abdurrahman (possible variant: Abd al-Rahman) planned to send suicide bombers to attack the embassies of the U.S., Germany, and Denmark in Kabul. The sensitive source with firsthand access to al-Qa,ida associates in Pakistan claimed the attack was not imminent and Abdurrahman was waiting for bombers to arrive from the Waziristan area, Federally Administered Tribal Areas, Pakistan. However, the vehicles to be used in the operation were ready in Kabul.

¶17. (S//NF) While DS/TIA/ITA cannot corroborate this reporting, it is of note that the ongoing plot to conduct suicide attacks against the U.S. Ambassador and Embassy in Kabul involves al-Qa,ida operatives. A name check on an al-Qa,ida-associated operative named Haji Abdurrahman was inconclusive. The stated possible variant, Abd al-Rahman, is used frequently. One possibility is that, since October 2007, bodies of credible reporting suggested senior al-Qa,ida leader Abdul Rehman al-Najdi is involved in targeting U.S. and European diplomatic facilities in Pakistan with missile and suicide attacks. Another possibility is Zubayr al-Misri (a.k.a. Wakas, Terrorist Identities Datamart Environment (TIDE) number 12467499), a known al-Qa,ida operative who uses the alias Abd al-Rahman Hussein Hilal. Finally, al-Qa,ida terrorist Ahmad Umar Abd al Rahman (TIDE number 47153), the son of the &Blind Sheikh8 Umar Abd Al-Rahman, is believed to have previously led rocket attacks against Shkin base in Paktika Province. (Appendix sources 6-8)

¶18. (S//REL TO USA, AUS, CAN, GBR, NZL) Afghanistan - Militants plan suicide operations in/around Kabul airport: Tearline states, &Afghan opposition elements were planning, as of mid-October, to organize and conduct suicide and sabotage operations against targets inside the Kabul airport and in the airport vicinity. The dates and the method of conducting the operations are unknown. The Afghan National Security Directorate warned the security forces and police of the potential attacks, bringing special attention to the following important, vulnerable points in the vicinity of the airport:
--UK headquarters, which is situated along the airport Customs Western Road, which ends in the square (NFI);
--the entry door and the internal enclosure, of the Triko company (spelling not verified);
--a guesthouse used by Americans which is located along the meteorology organization, road, south of the airport,s military police guard post;
--the entry to the airport, south of Sarparim (spelling not verified; NFI) along the airport Customs Western Road; and
--the area which contains oil reserves storehouses.8

¶19. (S//NF) DS/TIA/ITA notes it appears Afghan authorities mentioned these areas because of particular vulnerabilities rather than specific information denoting them as targets. Jalalabad Road and Airport Road lie in the vicinity of the airport. Direct fire and remote-controlled IEDs continue to plague convoys on Jalalabad Road. Militants have carried out six attacks against military and civilian convoys on Airport Road (a.k.a. Route White, Great Massoud) in the past two

years, with the latest being the March 13 suicide VBIED attack against a Coalition convoy. There are currently ongoing threats to ambush the U.S. Ambassador on Airport Road. The airport is typically targeted with rockets rather than suicide attacks; however, the increasing use of complex suicide attacks could breach the layers of security at the airport, such as the attack on the Ministry of Information and Culture on October 30 by one suicide bomber accompanied by one to two other militants with small arms to breach the facility. (Appendix source 9)

¶20. (S//NF) Afghanistan - Plans to kidnap UN employee in Konar Province: Lashkar-e-Tayyiba/Jama,at ud-Dawa (LT/JUD) commander Zia Rahman tasked Maulawi Ali Khan and 25 Taliban fighters to kidnap a UN employee who worked at a polling center in Shigal District, Konar Province. The developing source also indicated Khan planned to emplace three remote-controlled IEDs along the main road between Shigal and Asmar districts in Konar Province.

¶21. (S//NF) DS/TIA/ITA notes a recent tearline also suggested insurgents in Konar Province intended to target foreigner workers or possible Afghan working for foreign or Afghan Government entities: (S//REL TO USA, ISAF, NATO) &Taliban insurgents reportedly planned in early November a series of operations within Nawa, Sarkani District, and Khas Konar District. Within the Nawa region, the Taliban planned on emplacing mines along the road between Donai and Nawa in the hope of targeting Afghan and Coalition forces traveling along this route. They also planned on kidnapping road construction engineers and contractors. Further, Taliban insurgents also intended to either assassinate or kidnap foreign workers and Afghan Government employees in Sarkani and Khas Konar districts.8 Exposure of UN and Afghan workers to high-risk environments is likely to increase as the election registration process and preparations for elections continues into next year.

¶22. (S//NF) A name check on Maulawi Ali Khan indicates two possibly active insurgents in Konar. A sensitive source with secondhand access reported in late August 2007 that Taliban commander Ali Khan conducted a rocket attack in Asmar District, Konar Province. The source claimed Khan was the Taliban commander for Shigal, Asmar, Ghaziabad, Naray, and Dangam districts. In early September, the Afghan National Directorate of Security reported Maulawi Ali Khan participated in a meeting in Peshawar, Pakistan, in which Taliban military commander for Konar Province, Maulawi Najibullah, ordered attacks on Afghan security forces and the Coalition base in Asmar. Alternatively, a developing source reported in September 2007 that Maulawi Ali Khan Gujar from Naray District attended a meeting of Konar Province shura members in which an LT commander was also present. A name check on LT/JUD commander Zia Rahman was inconclusive. (Appendix sources 10-14)

¶23. (S//REL TO USA, FVEY) Afghanistan - Shooting of UN guard may mark end of security calm in affluent Kabul neighborhood: Tearline states, &The recent shooting of an unidentified Afghan guard on duty at a UN security post in Kabul,s Wazir Akbar Khan area may mark the end of a long quiet period in this area and is likely to have a significant impact on the security situation, according to informed sources in early November. Observers are concerned that the shooting, which was not fatal, may have been an act of retribution or carried out by a disgruntled individual. Non-governmental and international officials, as well as local businesses, are being warned to acknowledge the considerable dangers now present in Wazir Akbar Khan and through Kabul -- including kidnappings, shootings, and bombings -- and to refrain from circulating unarmed and unescorted.8

¶24. (S//NF) DS/TIA/ITA notes, while this shooting in an affluent area of Kabul is not a terrorist incident, it is indicative of the rise in crimes involving foreign entities and foreigners in Kabul city. The Afghanistan NGO Safety Office notes at least 18 incidents in Kabul Province this year in which insurgents and criminals have targeted

non-governmental organizations (NGOs), but not all included foreign nationals. Compared to previous years, there has been a consistently high volume of incidents against foreigners and an increased frequency in the deliberate targeting of foreigners. Most recently in Kabul, a female Canadian journalist was kidnapped, and a female British aid worker was assassinated. It is still unclear if the murder of the two DHL executives by a guard on October 25 was due to personal grievances or a planned criminal/insurgent assassination in connection with narcotics trafficking. (Appendix source 15)

¶25. (U) Cyber Threats

¶26. (U) Worldwide - Criminals capitalize on presidential election to launch spam campaign:

¶27. (U) Key highlights:
 A spam campaign was launched shortly after President-Elect Obama,s acceptance speech.
 The malicious e-mail messages sent appear to come from reputable news agencies.
 A link in the message directs users to a webpage similar to DoS, &America.gov.8
 Much of the spam traffic detected may have been generated by a single exploit.

¶28. (U) Source paragraph: &Experts at (computer security company) Sophos have discovered a widespread spam attack, claiming to contain a link to news about the new president. The e-mails, which have subject lines such as Obama win preferred in world poll, and claim to come from news@president.com, have accounted for approximately 60 percent of all malicious spam seen by SophosLabs in the last hour.8

¶29. (U) CTAD comment: As early as 2007, reports surfaced concerning malicious actors taking interest in exploiting the 2008 U.S. presidential elections. That year, hundreds of fraudulent websites were crafted to appear as legitimate sites belonging to the candidates. However, in reality, those websites were used to underhandedly distribute malicious software (malware) to unsuspecting Web surfers. Though the campaigning has concluded and the next U.S. President has been elected, cyber criminals have continued to exploit the occasion by launching a new campaign of their own. These malicious actors have constructed spam e-mail messages intended to take advantage of individuals interested in viewing videos relating to election news results, President-Elect Barack Obama,s acceptance speech, or interviews with Obama,s political advisers.

¶30. (U) CTAD comment: According to open source reporting, less than 12 hours after the acceptance speech was given, cyber criminals seeking to take advantage of unwary computer users fashioned a socially engineered malware attack surrounding the event. The e-mail messages carry a variety of enticing subject lines, many of them forged to appear to come from reputable news agencies such as Time Magazine, BBC, and CNN. The body of the messages contain a link purporting to send the recipient to the &election results news page,8 where they will be able to view the desired video; however, the link in fact directs the user to a webpage hosting an embedded video designed to look like the DoS, &America.gov8 site -- an online diplomacy tool that operates as a &platform for the Department, other agencies, the private sector, and civil society to engage in dialogue with international audiences.8 Of note, varying descriptions of attack specifics have been presented by leading computer security vendors Sophos, Websense, and Cloudmark; however, screen shots of the attacks provided by Cloudmark and Sophos are identical. Because of this discovery, computer security analysts have concluded this may be an indication that a great deal of the massive amount of malicious traffic seen is &being generated by a single exploit.8

¶31. (SBU) CTAD comment: After reaching the deceptive webpage, the user is instructed to click on a provided link to download Adobe Flash 9 in order to view the video. Selecting

this link initiates the process for infecting the user,s computer with a Trojan horse program that installs a &phishing kit8 onto the victim computer which is used to collect sensitive data from the compromised system. According to Websense, &major anti-virus vendors are not detecting this threat;8 however, Symantec anti-virus solutions deployed by the DoS do detect the malicious programs.

¶32. (SBU) CTAD comment: It is not new for cyber criminals to capitalize on popular current events to deceive users into unwittingly surrendering personal information. Nonetheless, the techniques used in their attacks are becoming increasingly sophisticated. The use of a website designed to appear as an official USG-sponsored site illustrated in the aforementioned attack is one of many tactics used to convince users the provided content is legitimate, ultimately increasing the likelihood of its success. CTAD strongly recommends users remain informed about current phishing scams and avoid clicking directly on links found on webpages and in e-mail messages. In addition, e-mail messages suspected of containing harmful links or attachments should be immediately reported to the information systems security officer (ISSO) in order to assist in the protection of DoS personnel, computer systems, and networks. (Sophos (http://www.sophos.com), Graham Cluley,s Blog, &The president-elect,s first malware campaign,8 November 5, 2008)

SECRET//NOFORN//MR
Full Appendix with sourcing available upon request.
RICE